Terms used **md5 sha sha1** Found **185** of **182,223**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 185 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Relevance scale

1 Exploration for advanced SoC design: An HMAC processor with integrated SHA-1 and MD5 algorithms

Mao-Yin Wang, Chih-Pin Su, Chih-Tsun Huang, Cheng-Wen Wu

January 2004 **Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair ASP-DAC '04 , Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair ASP-DAC '04**

Publisher: IEEE Press , IEEE Press

Full text available: pdf(60.57 KB) Publisher Site

Additional Information: full citation, abstract, references

Cryptographic algorithms are prevalent and important in digital communications and storage, e.g., both SHA-1 and MD5 algorithms are widely used hash functions in IPSec and SSL for checking the data integrity. In this paper, we propose a hardware architecture for the standard HMAC function that supports both. Our HMAC design automatically generates the padding words and reuses the key for consecutive HMAC jobs that use the same key. We have also implemented the HMAC design in silicon. Compared wi ...

2 Power modeling and optimization for embedded systems: Analyzing the energy consumption of security protocols

Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, Niraj K. Jha

August 2003 **Proceedings of the 2003 international symposium on Low power electronics and design**

Publisher: ACM Press

Full text available: pdf(271.69 KB)

Additional Information: full citation, abstract, references, citings, index terms

Security is critical to a wide range of wireless data applications and services. While several security mechanisms and protocols have been developed in the context of the wired Internet, many new challenges arise due to the unique characteristics of battery powered embedded systems. In this work, we focus on an important constraint of such devices -- battery life -- and examine how it is impacted by the use of security protocols.We present a comprehensive analysis of the energy requirements of a ...

Keywords: 3DES, AES, DES, DSA, Diffie-Hellman, ECC, RSA, SSL, cryptographic algorithms, embedded system, energy analysis, handheld, low-power, security, security protocols

3 Security in embedded systems: Design challenges

Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady

August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press

Full text available: pdf(3.67 MB) Additional Information: full citation, abstract, references, index terms, review

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are oft ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, security protocols, tamper resistance

4 Security: Analyzing and modeling encryption overhead for sensor network nodes

Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu
September 2003 **Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications**
Publisher: ACM Press
Full text available: pdf(254.57 KB) Additional Information: full citation, abstract, references, index terms

Recent research in sensor networks has raised security issues for small embedded devices. Security concerns are motivated by the deployment of a large number of sensory devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices. A mismatch between wide arithmetic for security (32 bit word operations) and embedded data bus widths (often only 8 or 16 bits) combined ...

Keywords: analysis, embedded systems, encryption overhead, model, sensor networks

5 A public-key based secure mobile IP

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent
October 1999 **Wireless Networks**, Volume 5 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

6 New technologies in system design: Divide-and-concatenate: an architecture level optimization technique for universal hash functions

Bo Yang, Ramesh Karri, David A. McGrew
June 2004 **Proceedings of the 41st annual conference on Design automation**
Publisher: ACM Press
Full text available: pdf(194.78 KB) Additional Information: full citation, abstract, references, index terms

We present an architecture optimization technique called divide-and-concatenate for universal hash functions. The area of a multiplier increases quadratically and its speed increases gradually with the operand size and two universal hash functions are equivalent if they have the same collision probability property. Based on these observations, the divide-and-concatenate approach divides a 2w-bit data path (with collision probability 2-2w) into two w-bit data paths (each with collision probabilit ...

Keywords: Design, Performance, Experimentation

7 Embedded applications: Encryption overhead in embedded systems and sensor network nodes: modeling and analysis

Ramnath Venugopalan, Prasanth Ganesan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu

October 2003 **Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems**

Publisher: ACM Press

Full text available: pdf(293.59 KB) Additional Information: full citation, abstract, references, citings, index terms

Recent research in sensor networks has raised issues of security for small embedded devices. Security concerns are motivated by the deployment of a large number of sensory devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices. A mismatch between wide arithmetic for security (32 bit word operations) and embedded data bus widths (often only 8 or 16 bits) combi ...

Keywords: embedded systems, encryption, security, sensor networks

8 Practical byzantine fault tolerance and proactive recovery

Miguel Castro, Barbara Liskov

November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4

Publisher: ACM Press

Full text available: pdf(1.63 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults. BFT can be used in practice to implement re ...

Keywords: Byzantine fault tolerance, asynchronous systems, proactive recovery, state machine replication, state transfer

9 Efficient Memory Integrity Verification and Encryption for Secure Processors

G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas Devadas

December 2003 **Proceedings of the 36th annual IEEE/ACM International Symposium on Microarchitecture**

Publisher: IEEE Computer Society

Full text available: pdf(307.01 KB) Additional Information: full citation, abstract, citings, index terms

Secure processors enable new sets of applications suchas commercial grid computing, software copy-protection,and secure mobile agents by providing security from bothphysical and software attacks. This paper proposes newhardware mechanisms for memory integrity verification andencryption, which are two key primitives required in single-chipsecure processors. The integrity verification mechanismoffers significant performance advantages over existingones when the checks are infrequent as in grid com ...

10 GnuPG hacks

Tony Stieber

March 2006 **Linux Journal**, Volume 2006 Issue 143

Publisher: Specialized Systems Consultants, Inc.

Full text available: html(23.22 KB) Additional Information: full citation, abstract, index terms

What can GnuPG do for you besides encrypt and decrypt e-mail?

11 Security processor design: Design and test of a scalable security processor

Chih-Pin Su, Chen-Hsing Wang, Kuo-Liang Cheng, Chih-Tsun Huang, Cheng-Wen Wu

January 2005 **Proceedings of the 2005 conference on Asia South Pacific design automation ASP-DAC '05**

Publisher: ACM Press

Full text available: pdf(319.90 KB) Additional Information: full citation, abstract, references

This paper presents a security processor to accelerate cryptographic processing in modern security applications. Our security processor is capable of popular cryptographic functions such as RSA, AES, hashing and random number generation, etc. With proposed Crypto-DMA controller, data gathering and scattering become flexible for security processing, using a simple descriptor-based programming model. The architecture of the security processor with its core-based platform is scalable and configurab ...

12 Feedback driven instruction-set extension

Uwe Kastens, Dinh Khoi Le, Adrian Slowik, Michael Thies

June 2004 **ACM SIGPLAN Notices , Proceedings of the 2004 ACM SIGPLAN/SIGBED conference on Languages, compilers, and tools for embedded systems LCTES '04**, Volume 39 Issue 7

Publisher: ACM Press

Full text available: pdf(525.86 KB) Additional Information: full citation, abstract, references, index terms

Application specific instruction-set processors combine an efficient general purpose core with special purpose functionality that is tailored to a particular application domain. Since the extension of an instruction set and its utilization are non-trivial tasks, sophisticated tools have to provide guidance and support during design. Feedback driven optimization allows for the highest level of specialization, but calls for a simulator that is aware of the newly proposed instructions, a compiler t ...

Keywords: codesign, compiler generation, encryption, instruction-set extensions, network processor, simulator generation

13 How to set up and use tripwire

Marco Fioretti

June 2006 **Linux Journal**, Volume 2006 Issue 146

Publisher: Specialized Systems Consultants, Inc.

Full text available: html(19.21 KB) Additional Information: full citation, abstract

Don't let intruders go unnoticed.

14 Embedded applications: AES and the cryptonite crypto processor

Dino Oliva, Rainer Buchty, Nevin Heintze

October 2003 **Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems**

Publisher: ACM Press

Full text available: pdf(346.09 KB) Additional Information: full citation, abstract, references, index terms

CRYPTONITE is a programmable processor tailored to the needs of crypto algorithms. The design of CRYPTONITE was based on an in-depth application analysis in which standard crypto algorithms (AES, DES, MD5, SHA-1, etc) were distilled down to their core functionality. We describe this methodology and use AES as a central example. Starting with a functional description of AES, we give a high level account of how to implement AES efficiently in hardware, and present several novel optimizations (whic ...

Keywords: AES, architecture, cryptography, high-bandwidth, high-speed, processor, round key generation, software implementation

15

Security protocols: Provably secure password-based authentication in TLS
Michel Abdalla, Emmanuel Bresson, Olivier Chevassut, Bodo Möller, David Pointcheval
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(378.65 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we show how to design an efficient, provably secure password-based authenticated key exchange mechanism specifically for the TLS (Transport Layer Security) protocol. The goal is to provide a technique that allows users to employ (short) passwords to securely identify themselves to servers. As our main contribution, we describe a new password-based technique for user authentication in TLS, called *Simple Open Key Exchange* (SOKE). Loosely speaking, the SOKE ciphersuites are un ...

Keywords: TLS, encrypted key exchange, password authentication

16 Crypto-based identifiers (CBIDs): Concepts and applications
Gabriel Montenegro, Claude Castelluccia
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: pdf(262.76 KB) Additional Information: full citation, abstract, references, index terms, review

This paper addresses the identifier ownership problem. It does so by using characteristics of Statistical Uniqueness and Cryptographic Verifiability (SUCV) of certain entities which this document calls SUCV Identifiers and Addresses, or, alternatively, Crypto-based Identifiers. Their characteristics allow them to severely limit certain classes of denial-of-service attacks and hijacking attacks. SUCV addresses are particularly applicable to solve the address ownership problem that hinders mechani ...

Keywords: Security, address ownership, authorization, group management, mobile IPv6, opportunistic encryption

17 Secret key distribution protocol using public key cryptography
Amit Parnerkar, Dennis Guster, Jayantha Herath
October 2003 **Journal of Computing Sciences in Colleges**, Volume 19 Issue 1
Publisher: Consortium for Computing Sciences in Colleges
Full text available: pdf(74.93 KB) Additional Information: full citation, abstract, references, index terms

This paper presents the description and analysis of a protocol, which uses hybrid crypto algorithms for key distribution. A triple DES with a 168-bit key is used to generate the secret key. This secret key is transferred with the help of public key cryptography. The authentication process is accomplished by using the message digest algorithm MD5. This protocol uses mutual authentication in which, both participants have to authenticate themselves via a third trusted certificate authority (CA). Th ...

18 Cryptography as an operating system service: A case study
Angelos D. Keromytis, Jason L. Wright, Theo De Raadt, Matthew Burnside
February 2006 **ACM Transactions on Computer Systems (TOCS)**, Volume 24 Issue 1
Publisher: ACM Press
Full text available: pdf(669.12 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic transformations are a fundamental building block in many security applications and protocols. To improve performance, several vendors market hardware accelerator cards. However, until now no operating system provided a mechanism that allowed both uniform and efficient use of this new type of resource.We present the OpenBSD Cryptographic Framework (OCF), a service virtualization layer implemented inside the operating system kernel, that provides uniform access to accelerator functio ...

Keywords: Encryption, authentication, cryptographic protocols, digital signatures, hash functions

19 Securing Mobile Appliances: New Challenges for the System Designer

Anand Raghunathan, Srivaths Ravi, Sunil Hattangady, Jean-Jacques Quisquater

March 2003 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '03**

Publisher: IEEE Computer Society

Full text available: pdf(257.28 KB) Publisher Site

Additional Information: full citation, abstract, index terms

As intelligent electronic systems pervade all aspects of our lives, capturing, storing, and communicating a wide range of sensitive and personal data, security is emerging as a critical concern that must be addressed in order to enable several current and future applications. Mobile appliances, which will play a critical role in enabling the visions of ubiquitous computing and communications, and ambient intelligence, are perhaps the most challenging to secure ¿ they often rely on a public mediu ...

20 Bayeux: an architecture for scalable and fault-tolerant wide-area data dissemination

Shelley Q. Zhuang, Ben Y. Zhao, Anthony D. Joseph, Randy H. Katz, John D. Kubiatowicz

January 2001 **Proceedings of the 11th international workshop on Network and operating systems support for digital audio and video**

Publisher: ACM Press

Full text available: pdf(272.26 KB) Additional Information: full citation, abstract, references, citings, index terms

The demand for streaming multimedia applications is growing at an incr edible rate. In this paper, we propose Bayeux, an efficient application-level multicast system that scales to arbitrarily large receiver groups while tolerating failures in routers and network links. Bayeux also includes specific mechanisms for load-balancing across replicate root nodes and more efficient bandwidth consumption. Our simulation results indicate that Bayeux maintains these properties while keeping transmi ...

Results 1 - 20 of 185 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Terms used **md5 sha sha1** Found **185** of **182,223**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 21 - 40 of 185 Result page: previous 1 **2** 3 4 5 6 7 8 9 10 next

Relevance scale

21 Using smartcards to secure a personalized gambling device

William A. Aiello, Aviel D. Rubin, Martin J. Strauss
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(762.94 KB) Additional Information: full citation, abstract, references, index terms

We introduce a technique for using an untrusted device, such as a hand-held personal digital assistant or a laptop to perform real financial transactions without a network. We utilize the tamper-resistant nature of smartcards to store value on them and perform probabilistic computations based on user input. We discuss an application of this to gambling. The technique has the properties that the user is guaranteed to make money when he wins and the house is guaranteed to make money w ...

22 Data mining, knowledge discovery & OLTP: Using secure coprocessors for privacy preserving collaborative data mining and analysis

Bishwaranjan Bhattacharjee, Naoki Abe, Kenneth Goldman, Bianca Zadrozny, Vamsavardhana R. Chillakuru, Marysabel del Carpio, Chid Apte
June 2006 **Proceedings of the 2nd international workshop on Data management on new hardware DaMoN '06**
Publisher: ACM Press
Full text available: pdf(248.64 KB) Additional Information: full citation, abstract, references, index terms

Secure coprocessors have traditionally been used as a keystone of a security subsystem, eliminating the need to protect the rest of the subsystem with physical security measures. With technological advances and hardware miniaturization they have become increasingly powerful. This opens up the possibility of using them for non traditional use. This paper describes a solution for privacy preserving data sharing and mining using cryptographically secure but resource limited coprocessors. It uses me ...

Keywords: collaboration, data mining, federation, privacy

23 Smart packets: applying active networks to network management

Beverly Schwartz, Alden W. Jackson, W. Timothy Strayer, Wenyi Zhou, R. Dennis Rockwell, Craig Partridge
February 2000 **ACM Transactions on Computer Systems (TOCS)**, Volume 18 Issue 1
Publisher: ACM Press
Full text available: pdf(190.33 KB) Additional Information: full citation, abstract, references, citings, index terms

This article introduces Smart Packets and describes the smart Packets architecture, the

packet formats, the language and its design goals, and security considerations. Smart Packets is an Active Networks project focusing on applying active networks technology to network management and monitoring. Messages in active networks are programs that are executed at nodes on the path to one or more target hosts. Smart Packets programs are written in a tightly encoded, safe language specifically des ...

Keywords: active networks

24 A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP)

Adam Stubblefield, John Ioannidis, Aviel D. Rubin

May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2

Publisher: ACM Press

Full text available: pdf(207.38 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we present a practical key recovery attack on WEP, the link-layer security protocol for 802.11b wireless networks. The attack is based on a partial key exposure vulnerability in the RC4 stream cipher discovered by Fluhrer, Mantin, and Shamir. This paper describes how to apply this flaw to breaking WEP, our implementation of the attack, and optimizations that can be used to reduce the number of packets required for the attack. We conclude that the 802.11b WEP standard is completely ...

Keywords: Wireless security, wired equivalent privacy

25 Identification and classification: Transport layer identification of P2P traffic

Thomas Karagiannis, Andre Broido, Michalis Faloutsos, Kc claffy

October 2004 **Proceedings of the 4th ACM SIGCOMM conference on Internet measurement**

Publisher: ACM Press

Full text available: pdf(540.18 KB) Additional Information: full citation, abstract, references, index terms

Since the emergence of peer-to-peer (P2P) networking in the late '90s, P2P applications have multiplied, evolved and established themselves as the leading `growth app' of Internet traffic workload. In contrast to first-generation P2P networks which used well-defined port numbers, current P2P applications have the ability to disguise their existence through the use of arbitrary ports. As a result, reliable estimates of P2P traffic require examination of packet payload, a methodological landmin ...

Keywords: measurements, peer-to-peer, traffic classification

26 Performance analysis of MD5

Joseph D. Touch

October 1995 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication SIGCOMM '95**, Volume 25 Issue 4

Publisher: ACM Press

Full text available: pdf(1.04 MB) Additional Information: full citation, abstract, references, citings, index terms

MD5 is an authentication algorithm proposed as the required implementation of the authentication option in IPv6. This paper presents an analysis of the speed at which MD5 can be implemented in software and hardware, and discusses whether its use interferes with high bandwidth networking. The analysis indicates that MD5 software currently runs at 85 Mbps on a 190 Mhz RISC architecture, a rate that cannot be improved more than 20-40%. Because MD5 processes the entire body of a packet, this data ra ...

27 Performance analysis of TLS Web servers

Cristian Coarfa, Peter Druschel, Dan S. Wallach

February 2006 **ACM Transactions on Computer Systems (TOCS)**, Volume 24 Issue 1
Publisher: ACM Press
Full text available: pdf(743.44 KB) Additional Information: full citation, abstract, references, index terms

TLS is the protocol of choice for securing today's e-commerce and online transactions but adding TLS to a Web server imposes a significant overhead relative to an insecure Web server on the same platform. We perform a comprehensive study of the performance costs of TLS. Our methodology is to profile TLS Web servers with trace-driven workloads, replace individual components inside TLS with no-ops, and measure the observed increase in server throughput. We estimate the relative costs of each TLS p ...

Keywords: Internet, RSA accelerator, TLS, e-commerce, secure Web servers

28 Lx: a technology platform for customizable VLIW embedded processing
Paolo Faraboschi, Geoffrey Brown, Joseph A. Fisher, Giuseppe Desoli, Fred Homewood
May 2000 **ACM SIGARCH Computer Architecture News , Proceedings of the 27th annual international symposium on Computer architecture ISCA '00**, Volume 28 Issue 2
Publisher: ACM Press
Full text available: pdf(344.41 KB) Additional Information: full citation, abstract, references, citings, index terms

Lx is a scalable and customizable VLIW processor technology platform designed by Hewlett-Packard and STMicroelectronics that allows variations in instruction issue width, the number and capabilities of structures and the processor instruction set. For Lx we developed the architecture and software from the beginning to support both scalability (variable numbers of identical processing resources) and customizability (special purpose resources). In this paper we consider the followi ...

29 Improving Cost, Performance, and Security of Memory Encryption and Authentication
Chenyu Yan, Daniel Englender, Milos Prvulovic, Brian Rogers, Yan Solihin
June 2006 **Proceedings of the 33rd International Symposium on Computer Architecture ISCA '06**
Publisher: IEEE Computer Society
Full text available: pdf(363.21 KB) Additional Information: full citation, abstract

Protection from hardware attacks such as snoopers and mod chips has been receiving increasing attention in computer architecture. This paper presents a new combined memory encryption/authentication scheme. Our new split counters for counter-mode encryption simultaneously eliminate counter overflow problems and reduce per-block counter size, and we also dramatically improve authentication performance and security by using the Galois/Counter Mode of operation (GCM), which leverages counter-mode en ...

30 Application 2: A compact FPGA implementation of the hash function whirlpool
Norbert Pramstaller, Christian Rechberger, Vincent Rijmen
February 2006 **Proceedings of the internation symposium on Field programmable gate arrays FPGA'06**
Publisher: ACM Press
Full text available: pdf(240.32 KB) Additional Information: full citation, abstract, references, index terms

Recent breakthroughs in cryptanalysis of standard hash functions like SHA-1 and MD5 raise the need for alternatives. A credible alternative to for instance SHA-1 or the SHA-2 family of hash functions is Whirlpool. Whirlpool is a hash function that has been evaluated and approved by NESSIE and is standardized by ISO/IEC. To the best of our knowledge only one FPGA implementation of Whirlpool has been published to date. This implementation is designed for high throughput rates requiring a considera ...

Keywords: FPGA, compact hardware implementation, hash function, whirlpool

31 Cryptosystem and analysis: Addressing the shortcomings of one-way chains
Roberto Di Pietro, Luigi V. Mancini, Antonio Durante, Vishwas Patil
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(341.59 KB) Additional Information: full citation, abstract, references, index terms

One-way hash chains have been the preferred choice, over the symmetric and asymmetric key cryptography, in security setups where efficiency mattered; despite the ephemeral confidentiality and authentication they assure. Known constructions of one-way chains (for example, SHA-1 based), only ensure the forward secrecy and have limitations over their length i.e., a priori knowledge of chain's length is necessary before constructing it. In this paper, we will see how our approach, based on chameleon ...

Keywords: chameleon hash, one-way chain, secure group management for multicast

32 Signed kernel modules
Greg Kroah-Hartman
January 2004 **Linux Journal**, Volume 2004 Issue 117
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(21.05 KB) Additional Information: full citation, abstract

Crypto techniques give device drivers a new security check.

33 Operating systems security: Attestation-based policy enforcement for remote access
Reiner Sailer, Trent Jaeger, Xiaolan Zhang, Leendert van Doorn
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(261.52 KB) Additional Information: full citation, abstract, references, index terms

Intranet access has become an essential function for corporate users. At the same time, corporation's security administrators have little ability to control access to corporate data once it is released to remote clients. At present, no confidentiality or integrity guarantees about the remote access clients are made, so it is possible that an attacker may have compromised a client process and is now downloading or modifying corporate data. Even though we have corporate-wide access control over ...

Keywords: remote access, security management, trusted computing

34 A public-key based secure mobile IP
John Zao, Stephen Kent, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra
September 1997 **Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking**
Publisher: ACM Press
Full text available: pdf(1.95 MB) Additional Information: full citation, references, citings

35 Separating key management from file system security
David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel
December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5
Publisher: ACM Press
Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

36 Mobile Code and Distributed Systems: A new approach to DNS security (DNSSEC)

Giuseppe Ateniese, Stefan Mangard

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Publisher: ACM Press

Full text available: pdf(600.56 KB) Additional Information: full citation, abstract, references, index terms

The Domain Name System (DNS) is a distributed database that allows convenient storing and retrieving of resource records. DNS has been extended to provide security services (DNSSEC) mainly through public-key cryptography. We propose a new approach to DNSSEC that may result in a significantly more efficient protocol. We introduce a new strategy to build chains of trust from root servers to authoritative servers. The techniques we employ are based on symmetric-key cryptography.

Keywords: authentication protocols, digital signatures, domain name system security (DNSSEC), symmetric encryption

37 Random oracles are practical: a paradigm for designing efficient protocols

Mihir Bellare, Phillip Rogaway

December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.17 MB) Additional Information: full citation, abstract, references, citings, index terms

We argue that the random oracle model—where all parties have access to a public random oracle—provides a bridge between cryptographic theory and cryptographic practice. In the paradigm we suggest, a practical protocol P is produced by first devising and proving correct a protocol PR for the random oracle model, and then replacing oracle accesses by the computation of an "appropriately chosen" function h

38 Secure names for bit-strings

Stuart Haber, W. Scott Stornetta

April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(968.22 KB) Additional Information: full citation, references, index terms

39 Wide-area architecture and protocols: Hierarchical substring caching for efficient content distribution to low-bandwidth clients

Utku Irmak, Torsten Suel

May 2005 **Proceedings of the 14th international conference on World Wide Web**

Publisher: ACM Press

Full text available: pdf(221.09 KB) Additional Information: full citation, abstract, references, index terms

While overall bandwidth in the internet has grown rapidly over the last few years, and an increasing number of clients enjoy broadband connectivity, many others still access the internet over much slower dialup or wireless links. To address this issue, a number of techniques for optimized delivery of web and multimedia content over slow links have been proposed, including protocol optimizations, caching, compression, and multimedia transcoding, and several large ISPs have recently begun to widel ...

Keywords: HTTP, WWW, compression, web caching, web proxies

40 Special session on security on SoC: Securing wireless data: system architecture challenges

Srivaths Ravi, Anand Raghunathan, Nachiketh Potlapally
October 2002 **Proceedings of the 15th international symposium on System Synthesis**
Publisher: ACM Press

Full text available: pdf(172.35 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is critical to a wide range of current and future wireless data applications and services. This paper highlights the challenges posed by the need for security during system architecture design for wireless handsets, and provides an overview of emerging techniques to address them. We focus on the computational requirements for securing wireless data transactions, revealing a gap between these requirements and the trends in processing capabilities of embedded processors used in wireless h ...

Keywords: 3DES, AES, DES, IPSec, RSA, SSL, WTLS, decryption, design methodology, embedded system, encryption, handset, mobile computing, performance, platform, security, security processing, system architecture, wireless communications

Terms used **universal hash md5 sha1** Found **1,916** of **182,223**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 New technologies in system design: Divide-and-concatenate: an architecture level optimization technique for universal hash functions
Bo Yang, Ramesh Karri, David A. McGrew
June 2004 **Proceedings of the 41st annual conference on Design automation**
Publisher: ACM Press
Full text available: pdf(194.78 KB) Additional Information: full citation, abstract, references, index terms

We present an architecture optimization technique called divide-and-concatenate for universal hash functions. The area of a multiplier increases quadratically and its speed increases gradually with the operand size and two universal hash functions are equivalent if they have the same collision probability property. Based on these observations, the divide-and-concatenate approach divides a 2w-bit data path (with collision probability 2-2w) into two w-bit data paths (each with collision probabilit ...

Keywords: Design, Performance, Experimentation

2 High-level techniques for specific applications: Power optimization for universal hash function data path using divide-and-concatenate technique
Bo Yang, Ramesh Karri
September 2005 **Proceedings of the 3rd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis CODES+ISSS '05**
Publisher: ACM Press
Full text available: pdf(194.62 KB) Additional Information: full citation, abstract, references, index terms

We present an architecture level low power design technique called divide-and-concatenate for universal hash functions based on the following observations: (i) the power consumption of a w-bit array multiplier and associated universal hash data path decreases as $O(w^4)$ if its clock rate remains constant. (ii) two universal hash functions are equivalent if they have the same collision probability property. In the proposed approach we divide a w-bit data path (with collision probability ...

Keywords: divide-and-concatenate, power optimization, universal hash function

3 T1-B: computer and network security symposium: Simple voice security protocol
Carole Bassil, Ahmed Serhrouchni, Nicolas Rouhana
July 2006 **Proceeding of the 2006 international conference on Communications and mobile computing IWCMC '06**
Publisher: ACM Press
Full text available: pdf(306.57 KB) Additional Information: full citation, abstract, references, index terms

The public telephone network has been evolving from manually switching wires carrying analog encoded voice to an automatically switched grid of copper-wired, fiber optical and wireless mobile connectivity carrying digitally encoded voice, image and data. The evolution of the information technology yields to a converged data and voice network based on IP technology. VoIP emerged and it is taking a large part of the telephony market nowadays. However, the IP network presents security threats to bo ...

Keywords: SVSP, security mechanisms, security services, telephony

4 Crypto-based identifiers (CBIDs): Concepts and applications

Gabriel Montenegro, Claude Castelluccia

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(262.76 KB) Additional Information: full citation, abstract, references, index terms, review

This paper addresses the identifier ownership problem. It does so by using characteristics of Statistical Uniqueness and Cryptographic Verifiability (SUCV) of certain entities which this document calls SUCV Identifiers and Addresses, or, alternatively, Crypto-based Identifiers. Their characteristics allow them to severely limit certain classes of denial-of-service attacks and hijacking attacks. SUCV addresses are particularly applicable to solve the address ownership problem that hinders mechani ...

Keywords: Security, address ownership, authorization, group management, mobile IPv6, opportunistic encryption

5 A public-key based secure mobile IP

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent

October 1999 **Wireless Networks**, Volume 5 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

6 Practical byzantine fault tolerance and proactive recovery

Miguel Castro, Barbara Liskov

November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4

Publisher: ACM Press

Full text available: pdf(1.63 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults. BFT can be used in practice to implement re ...

Keywords: Byzantine fault tolerance, asynchronous systems, proactive recovery, state machine replication, state transfer

7 Web technologies and applications (WTA): Migration to web services oriented architecture: a case study

Jia Zhang, Jen-Yao Chung, Carl K. Chang

March 2004 **Proceedings of the 2004 ACM symposium on Applied computing**

Publisher: ACM Press

Full text available: pdf(159.22 KB) Additional Information: full citation, abstract, references, citings, index terms

The rapid emerging of web-services technology is dramatically changing the scenario of web application design and development. This paper presents a web-services oriented architecture. As a case study, the paper reports on an on-going project on the design and development of a pass-through authentication web-services for on-line electronic payment applications. This is a first step towards an electronic payment web-service.

Keywords: Web application development, case study, software architecture, web services oriented architecture

8 A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP)

Adam Stubblefield, John Ioannidis, Aviel D. Rubin

May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2

Publisher: ACM Press

Full text available: pdf(207.38 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we present a practical key recovery attack on WEP, the link-layer security protocol for 802.11b wireless networks. The attack is based on a partial key exposure vulnerability in the RC4 stream cipher discovered by Fluhrer, Mantin, and Shamir. This paper describes how to apply this flaw to breaking WEP, our implementation of the attack, and optimizations that can be used to reduce the number of packets required for the attack. We conclude that the 802.11b WEP standard is completely ...

Keywords: Wireless security, wired equivalent privacy

9 Cryptography as an operating system service: A case study

Angelos D. Keromytis, Jason L. Wright, Theo De Raadt, Matthew Burnside

February 2006 **ACM Transactions on Computer Systems (TOCS)**, Volume 24 Issue 1

Publisher: ACM Press

Full text available: pdf(669.12 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic transformations are a fundamental building block in many security applications and protocols. To improve performance, several vendors market hardware accelerator cards. However, until now no operating system provided a mechanism that allowed both uniform and efficient use of this new type of resource.We present the OpenBSD Cryptographic Framework (OCF), a service virtualization layer implemented inside the operating system kernel, that provides uniform access to accelerator functio ...

Keywords: Encryption, authentication, cryptographic protocols, digital signatures, hash functions

10 Exploration for advanced SoC design: An HMAC processor with integrated SHA-1 and MD5 algorithms

Mao-Yin Wang, Chih-Pin Su, Chih-Tsun Huang, Cheng-Wen Wu

January 2004 **Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair ASP-DAC '04 , Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair ASP-DAC '04**

Publisher: IEEE Press , IEEE Press

Full text available: pdf(60.57 KB) Publisher Site Additional Information: full citation, abstract, references

Cryptographic algorithms are prevalent and important in digital communications and storage, e.g., both SHA-1 and MD5 algorithms are widely used hash functions in IPSec

and SSL for checking the data integrity. In this paper, we propose a hardware architecture for the standard HMAC function that supports both. Our HMAC design automatically generates the padding words and reuses the key for consecutive HMAC jobs that use the same key. We have also implemented the HMAC design in silicon. Compared wi ...

11 Perfectly one-way probabilistic hash functions (preliminary version)

Ran Canetti, Daniele Micciancio, Omer Reingold

May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing**

Publisher: ACM Press

Full text available: pdf(1.37 MB) Additional Information: full citation, references, citings, index terms

12 Hash-based IP traceback

Alex C. Snoeren

August 2001 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '01**, Volume 31 Issue 4

Publisher: ACM Press

Full text available: pdf(179.03 KB) Additional Information: full citation, abstract, references, citings, index terms

The design of the IP protocol makes it difficult to reliably identify the originator of an IP packet. Even in the absence of any deliberate attempt to disguise a packet's origin, wide-spread packet forwarding techniques such as NAT and encapsulation may obscure the packet's true source. Techniques have been developed to determine the source of large packet flows, but, to date, no system has been presented to track individual packets in an efficient, scalable fashion.We present a hash-based techn ...

13 Embedded applications: Encryption overhead in embedded systems and sensor network nodes: modeling and analysis

Ramnath Venugopalan, Prasanth Ganesan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu

October 2003 **Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems**

Publisher: ACM Press

Full text available: pdf(293.59 KB) Additional Information: full citation, abstract, references, citings, index terms

Recent research in sensor networks has raised issues of security for small embedded devices. Security concerns are motivated by the deployment of a large number of sensory devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices. A mismatch between wide arithmetic for security (32 bit word operations) and embedded data bus widths (often only 8 or 16 bits) combi ...

Keywords: embedded systems, encryption, security, sensor networks

14 Security: Analyzing and modeling encryption overhead for sensor network nodes

Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu

September 2003 **Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications**

Publisher: ACM Press

Full text available: pdf(254.57 KB) Additional Information: full citation, abstract, references, index terms

Recent research in sensor networks has raised security issues for small embedded devices. Security concerns are motivated by the deployment of a large number of sensory

devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices. A mismatch between wide arithmetic for security (32 bit word operations) and embedded data bus widths (often only 8 or 16 bits) combined ...

Keywords: analysis, embedded systems, encryption overhead, model, sensor networks

15 Application 2: A compact FPGA implementation of the hash function whirlpool

Norbert Pramstaller, Christian Rechberger, Vincent Rijmen

February 2006 **Proceedings of the internation symposium on Field programmable gate arrays FPGA'06**

Publisher: ACM Press

Full text available: pdf(240.32 KB) Additional Information: full citation, abstract, references, index terms

Recent breakthroughs in cryptanalysis of standard hash functions like SHA-1 and MD5 raise the need for alternatives. A credible alternative to for instance SHA-1 or the SHA-2 family of hash functions is Whirlpool. Whirlpool is a hash function that has been evaluated and approved by NESSIE and is standardized by ISO/IEC. To the best of our knowledge only one FPGA implementation of Whirlpool has been published to date. This implementation is designed for high throughput rates requiring a considera ...

Keywords: FPGA, compact hardware implementation, hash function, whirlpool

16 Lookups: Fast hash table lookup using extended bloom filter: an aid to network processing

Haoyu Song, Sarang Dharmapurikar, Jonathan Turner, John Lockwood

August 2005 **Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '05**

Publisher: ACM Press

Full text available: pdf(338.54 KB) Additional Information: full citation, abstract, references, index terms

Hash tables are fundamental components of several network processing algorithms and applications, including route lookup, packet classification, per-flow state management and network monitoring. These applications, which typically occur in the data-path of high-speed routers, must process and forward packets with little or no buffer, making it important to maintain wire-speed throughout. A poorly designed hash table can critically affect the worst-case throughput of an application, since the num ...

Keywords: forwarding, hash table

17 Power modeling and optimization for embedded systems: Analyzing the energy consumption of security protocols

Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, Niraj K. Jha

August 2003 **Proceedings of the 2003 international symposium on Low power electronics and design**

Publisher: ACM Press

Full text available: pdf(271.69 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is critical to a wide range of wireless data applications and services. While several security mechanisms and protocols have been developed in the context of the wired Internet, many new challenges arise due to the unique characteristics of battery powered embedded systems. In this work, we focus on an important constraint of such devices -- battery life -- and examine how it is impacted by the use of security protocols.We present a comprehensive analysis of the energy requirements of a ...

Keywords: 3DES, AES, DES, DSA, Diffie-Hellman, ECC, RSA, SSL, cryptographic algorithms, embedded system, energy analysis, handheld, low-power, security, security

protocols

18 Wide-area architecture and protocols: Hierarchical substring caching for efficient content distribution to low-bandwidth clients
Utku Irmak, Torsten Suel
May 2005 **Proceedings of the 14th international conference on World Wide Web**
Publisher: ACM Press
Full text available: pdf(221.09 KB) Additional Information: full citation, abstract, references, index terms

While overall bandwidth in the internet has grown rapidly over the last few years, and an increasing number of clients enjoy broadband connectivity, many others still access the internet over much slower dialup or wireless links. To address this issue, a number of techniques for optimized delivery of web and multimedia content over slow links have been proposed, including protocol optimizations, caching, compression, and multimedia transcoding, and several large ISPs have recently begun to widel ...

Keywords: HTTP, WWW, compression, web caching, web proxies

19 The random oracle methodology, revisited
Ran Canetti, Oded Goldreich, Shai Halevi
July 2004 **Journal of the ACM (JACM)**, Volume 51 Issue 4
Publisher: ACM Press
Full text available: pdf(334.81 KB) Additional Information: full citation, abstract, references, index terms

We take a critical look at the relationship between the security of cryptographic schemes in the Random Oracle Model, and the security of the schemes that result from implementing the random oracle by so called "cryptographic hash functions".The main result of this article is a negative one: There exist signature and encryption schemes that are secure in the Random Oracle Model, but for which *any implementation* of the random oracle results in insecure schemes. In the process of devising t ...

Keywords: CS-proofs, Correlation intractability, cryptography, diagonalization, the random-oracle model

20 Single-packet IP traceback
Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Beverly Schwartz, Stephen T. Kent, W. Timothy Strayer
December 2002 **IEEE/ACM Transactions on Networking (TON)**, Volume 10 Issue 6
Publisher: IEEE Press
Full text available: pdf(528.41 KB) Additional Information: full citation, abstract, references, citings, index terms

The design of the IP protocol makes it difficult to reliably identify the originator of an IP packet. Even in the absence of any deliberate attempt to disguise a packet's origin, widespread packet forwarding techniques such as NAT and encapsulation may obscure the packet's true source. Techniques have been developed to determine the source of large packet flows, but, to date, no system has been presented to track individual packets in an efficient, scalable fashion. We present a hash-based techn ...

Keywords: IP traceback, computer network management, computer network security, denial of service (DoS), network fault diagnosis, wide-area networks (WANs)

Thu, 27 Jul 2006, 2:30:27 PM EST

Edit an existing query or compose a new query in the Search Query Display.

Select a search number (#) to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

Search Query Display

Run Search Reset

Recent Search Queries

#1 ((md5 sha sha1)<in>metadata)

#2 ((md5 sha sha1)<in>metadata)

#3 ((md5 sha1)<in>metadata)

#4 ((md5 sha1)<in>metadata)

#5 sha sha1 md5

#6 (sha1 md5<IN>metadata)

#7 sha sha1 md5

#8 sha1 md5

Clear Session History

md5 sha1 circuit Advanced Search

Search using: MSN Ask.com Google

CUSTOM WEB FILTERS [Edit this Search]
Date: **Before November 29 2000**

WEB RESULTS by (Showing Results 1 - 10 of 266)

1. Random Noise Sources
Circuit designs for analog white noise sources ... This is best accomplished with a cryptographic hash, such as **MD5**, **SHA1** or RIPEM.
http://world.std.com/~reinhold/truenoise.html

2. Source package: 3270 Package: xfonts-x3270-misc Description: Font
... acs Description: Al's **Circuit** Simulator ACS is a general purpose **circuit** simulator.
http://ftp-master.debian.org/crypto-in-main/archive_contents.txt

3. Architecture: sparc Source: 3dwm Version: 0.3.1-8 Depends: libc6
Architecture: sparc Source: 3dwm Version: 0.3.1-8 Depends: libc6 (>= 2.2.4-4), libnobel (>= 0.3.1), omniorb (>= 3.0) Filename: pool/main/3/3dwm/3dwm-
http://www.unizar.es/softlibre/debian/dists/woody/main/binary-sparc/Pa...

4. Architecture: arm Version: 0.09-1 Depends: libc6 (>= 2.2.4-4)
93118672fc69bde7df568718f2649cb8 Description: Al's **Circuit** Simulator -- dummy package acs, Al's **Circuit** Simulator ...
http://www.scl.ameslab.gov/debian/dists/woody/main/binary-arm/Packages

5. Architecture: alpha Source: 3dwm Version: 0.3.1-8 Depends: libc6.1
Architecture: alpha Source: 3dwm Version: 0.3.1-8 Depends: libc6.1 (>= 2.2.4-4), libnobel (>= 0.3.1), omniorb (>= 3.0) Filename: pool/main/3/3dwm/
http://www.scl.ameslab.gov/debian/dists/woody/main/binary-alpha/Packag...

6. CompUSA Electronics: Shop at CompUSA for Computers, Televisions, ...
Algorithms Support Supports **MD5**, **SHA1**, HMAC-**MD5** and HMAC-**SHA1** Authentication Protocols

Supports PAP (Password Authentication ...
http://members.lycos.co.uk/pixicon/compusa-rebate/compusa-online-816.h...

7. IT Manager
... teleworker?s residence as a DSL **circuit** operating over a copper twisted pair. ... then onto a dedicated **circuit** to the customer?s ...
http://www.corecom.com/external/covadsec/covadsec.pdf

8. Architecture: s390 Version: 0.2.2-1 Depends: libc6 (>= 2.2.5-13)
Architecture: s390 Source: 3dwm Version: 0.3.1-11 Depends: libc6 (>= 2.2.4-4), libnobel (>= 0.3.1), libmeshio0, omniorb (>= 3.0) Filename: pool/main/
http://www.andrews.edu/debian/dists/unstable/main/binary-s390/Packages

9. Dec 99, Release Notes for BayRS Version 14.00
... the use or application of the product(s) or **circuit** layout(s) described herein.
http://www25.nortelnetworks.com/library/tpubs/pdf/router/soft1400/3086...

10. FEB 00, Release Notes for BayRS Version 14.10 for the Passport 5430 ...
... the use or application of the product(s) or **circuit** layout(s) described herein.
http://www25.nortelnetworks.com/library/tpubs/pdf/router/soft1410/3086...

« **Previous 1** 2 3 4 5 6 7 8 9 10 **Next** »

Search for "**md5 sha1 circuit**" using: MSN Google